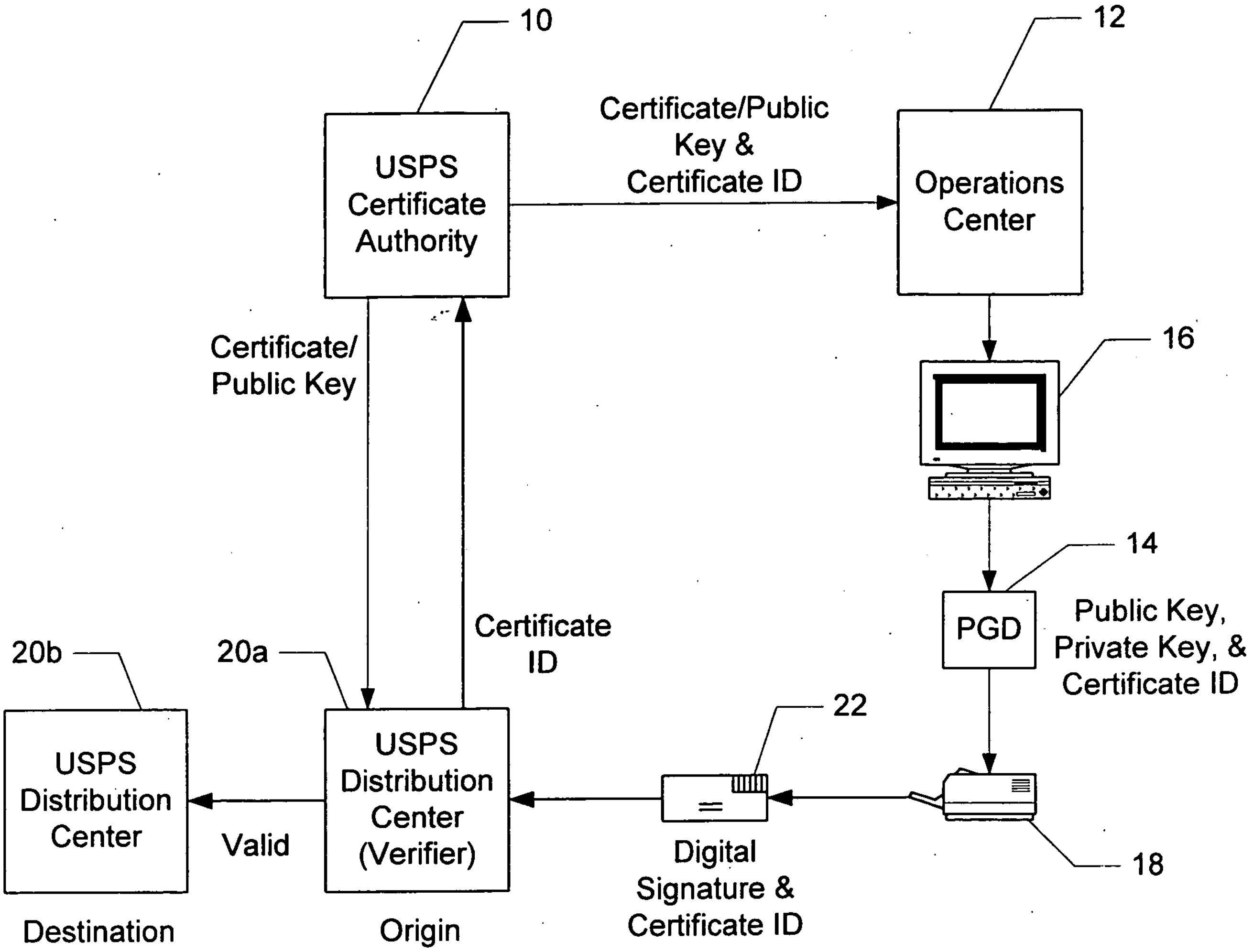

10
USPS Certificate Authority
Certificate/Public Key & Certificate ID
12
Operations Center
16
Certificate/ Public Key
14
PGD
Public Key, Private Key, & Certificate ID
Certificate ID
20b
20a
22
USPS Distribution Center
USPS Distribution Center (Verifier)
Valid
Digital Signature & Certificate ID
18
Destination
Origin

PRIOR ART

FIG. 1

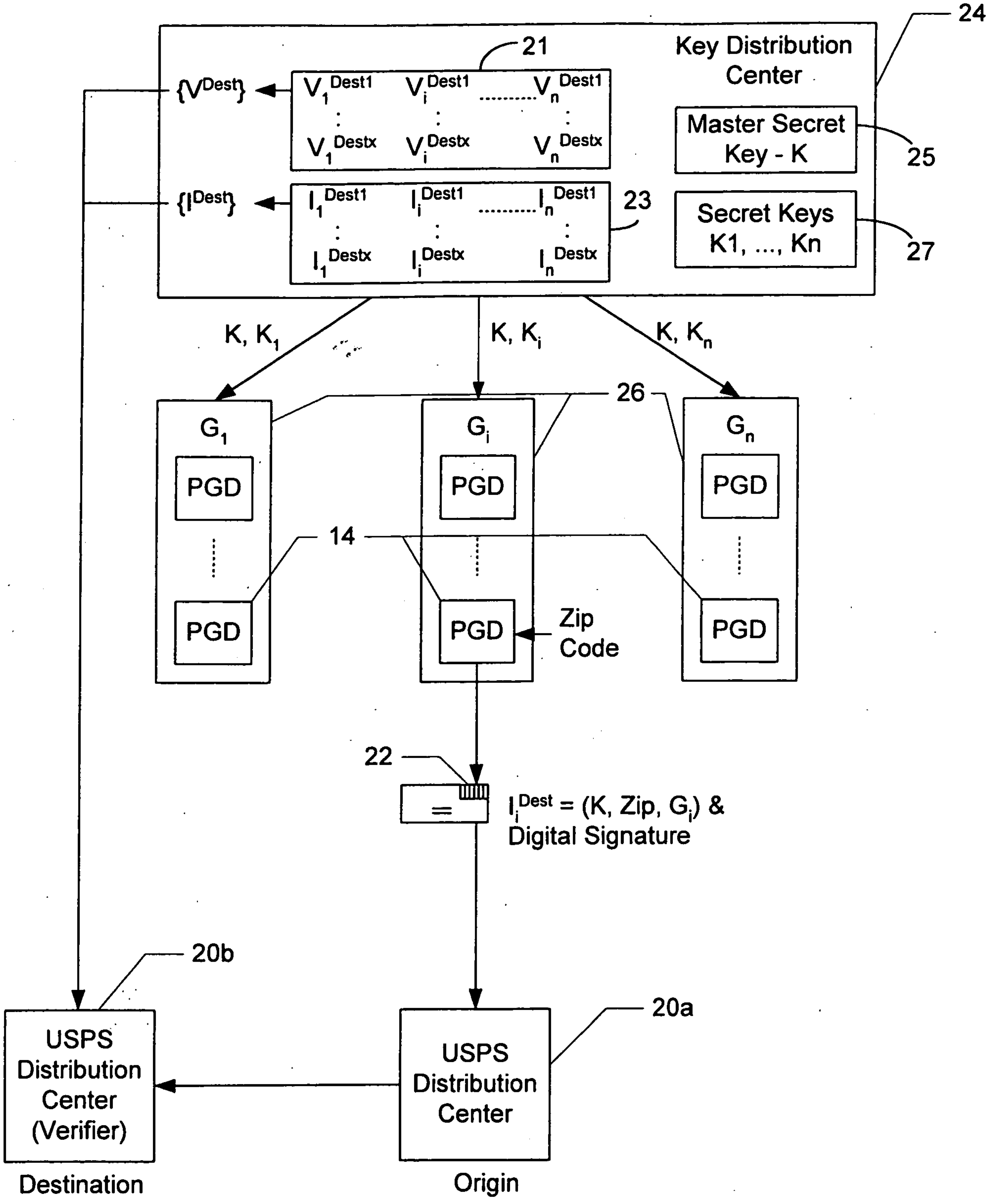
24
Key Distribution Center
21
$\{V^{Dest}\}$
V_1^{Dest1} V_i^{Dest1} .... V_n^{Dest1}
V_1^{Destx} V_i^{Destx} V_n^{Destx}
Master Secret Key - K
25
$\{I^{Dest}\}$
I_1^{Dest1} I_i^{Dest1} .... I_n^{Dest1}
I_1^{Destx} I_i^{Destx} I_n^{Destx}
23
Secret Keys K1, ..., Kn
27
K, K_1
K, K_i
K, K_n
26
G_1
G_i
G_n
PGD
PGD
PGD
14
PGD
PGD
PGD
Zip Code
22
$I_i^{Dest} = (K, Zip, G_i)$ & Digital Signature
20b
USPS Distribution Center (Verifier)
Destination
20a
USPS Distribution Center
Origin

FIG. 2

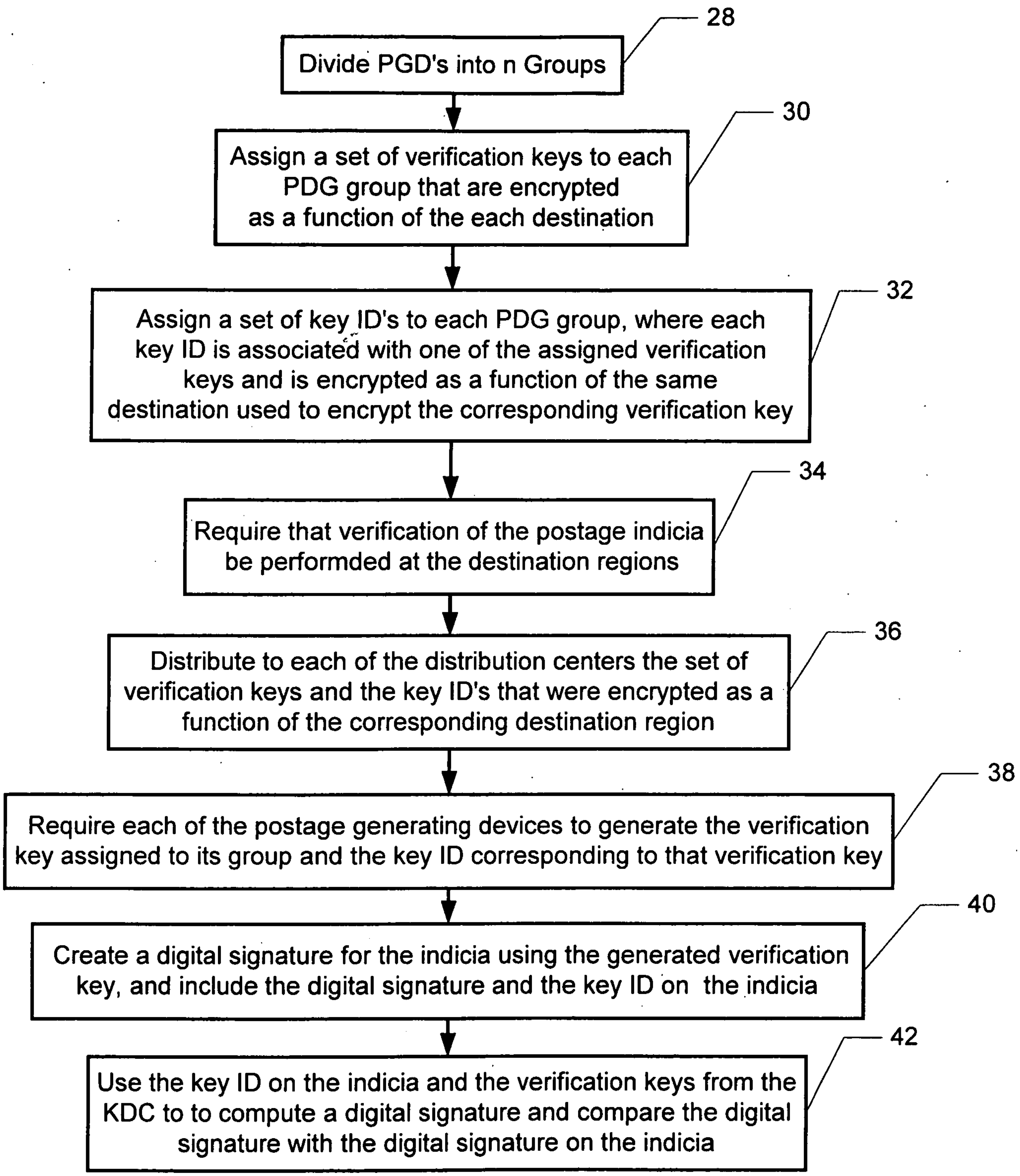
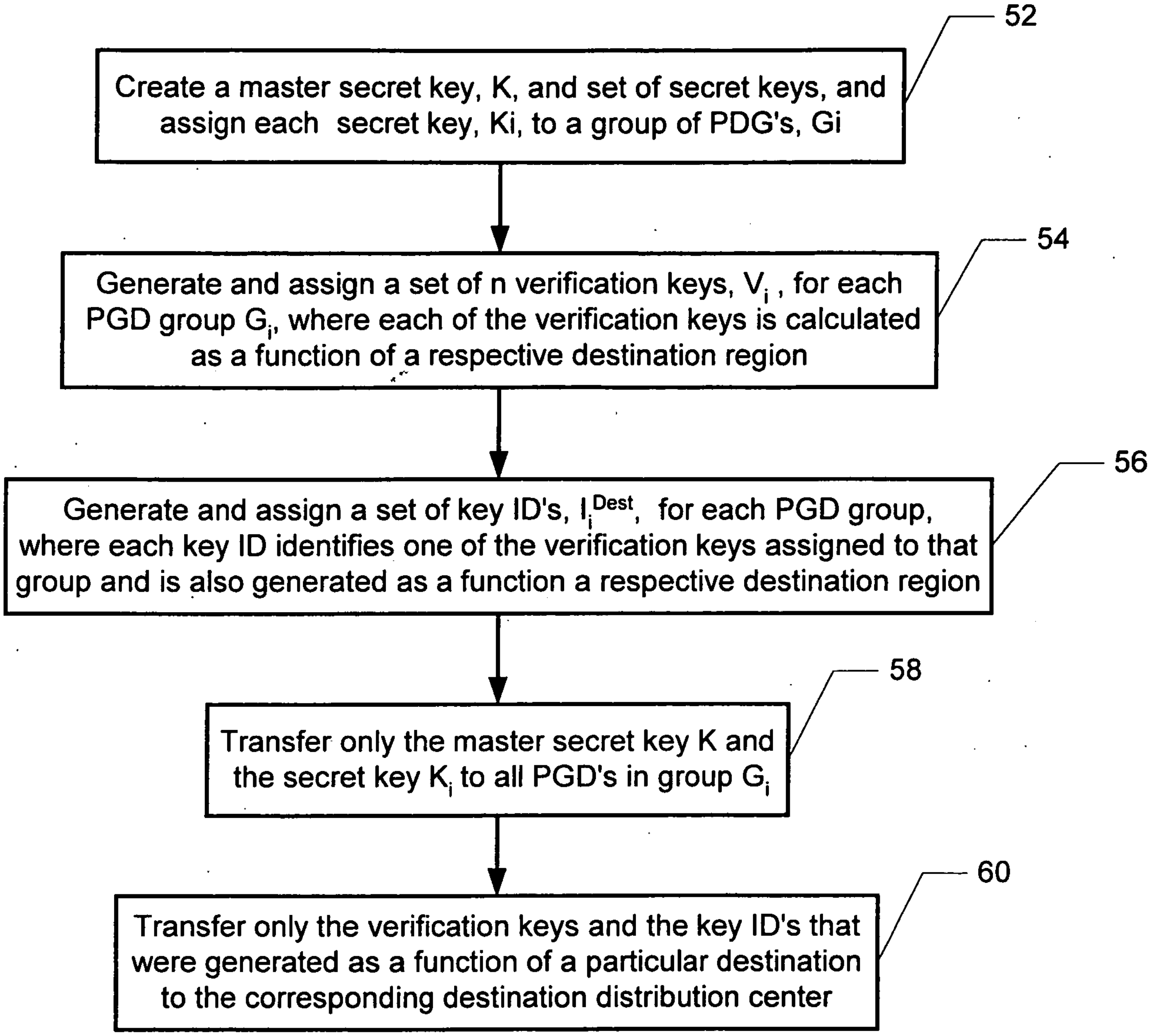
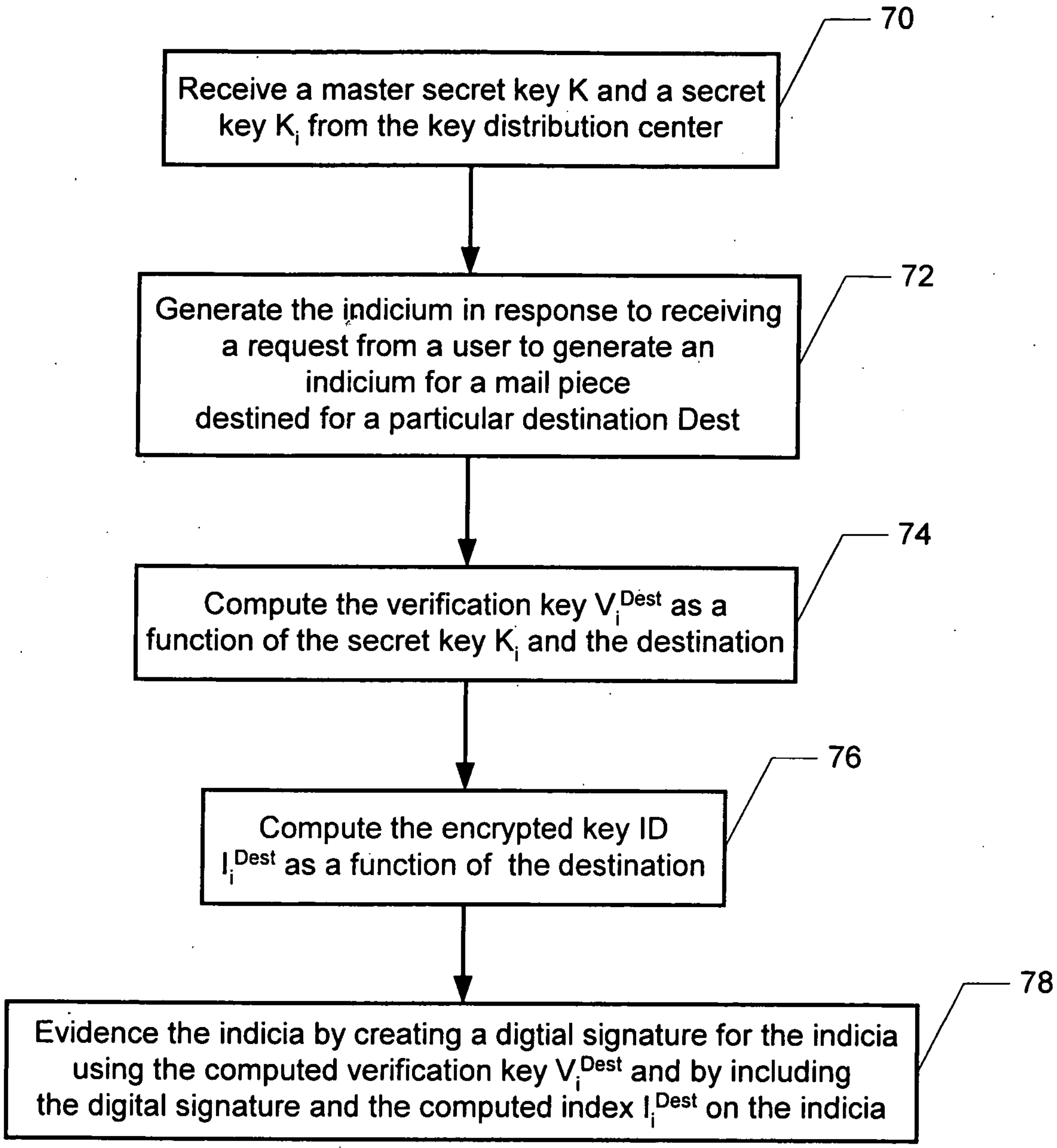

28
Divide PGD's into n Groups
30
Assign a set of verification keys to each PDG group that are encrypted as a function of the each destination
32
Assign a set of key ID's to each PDG group, where each key ID is associated with one of the assigned verification keys and is encrypted as a function of the same destination used to encrypt the corresponding verification key
34
Require that verification of the postage indicia be performded at the destination regions
36
Distribute to each of the distribution centers the set of verification keys and the key ID's that were encrypted as a function of the corresponding destination region
38
Require each of the postage generating devices to generate the verification key assigned to its group and the key ID corresponding to that verification key
40
Create a digital signature for the indicia using the generated verification key, and include the digital signature and the key ID on the indicia
42
Use the key ID on the indicia and the verification keys from the KDC to to compute a digital signature and compare the digital signature with the digital signature on the indicia

FIG. 3


52
Create a master secret key, K, and set of secret keys, and assign each secret key, Ki, to a group of PDG's, Gi
54
Generate and assign a set of n verification keys, V_i , for each PGD group G_i, where each of the verification keys is calculated as a function of a respective destination region
56
Generate and assign a set of key ID's, I_i^{Dest}, for each PGD group, where each key ID identifies one of the verification keys assigned to that group and is also generated as a function a respective destination region
58
Transfer only the master secret key K and the secret key K_i to all PGD's in group G_i
60
Transfer only the verification keys and the key ID's that were generated as a function of a particular destination to the corresponding destination distribution center

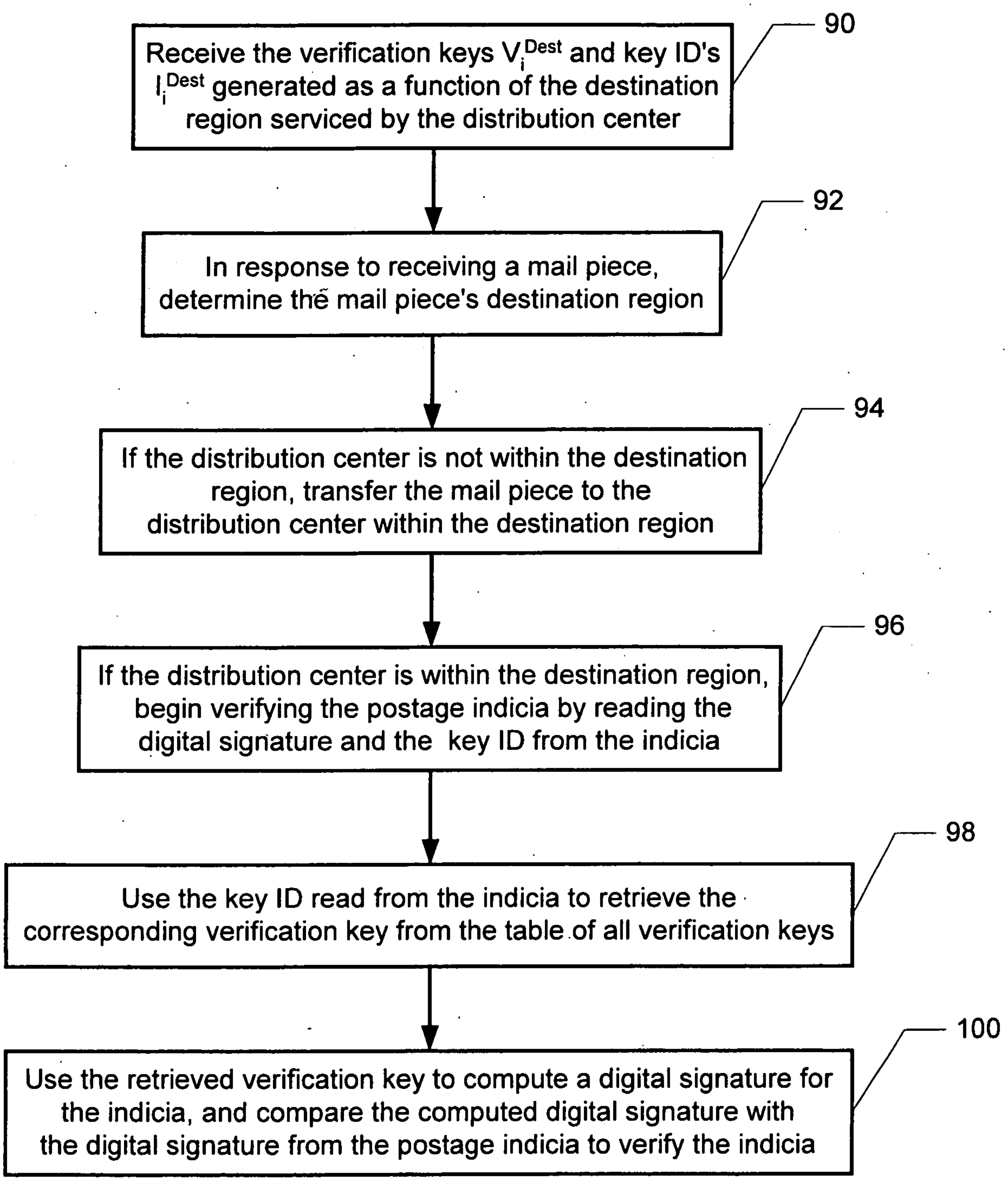
Generation and
Distribution of Keys

FIG. 4


70
Receive a master secret key K and a secret key K_i from the key distribution center
72
Generate the indicium in response to receiving a request from a user to generate an indicium for a mail piece destined for a particular destination Dest
74
Compute the verification key V_i^{Dest} as a function of the secret key K_i and the destination
76
Compute the encrypted key ID I_i^{Dest} as a function of the destination
78
Evidence the indicia by creating a digtial signature for the indicia using the computed verification key V_i^{Dest} and by including the digital signature and the computed index I_i^{Dest} on the indicia

Dispensing & Evidencing
Postage Indicia

FIG. 5



Receive the verification keys V_i^{Dest} and key ID's I_i^{Dest} generated as a function of the destination region serviced by the distribution center
90
In response to receiving a mail piece, determine the mail piece's destination region
92
If the distribution center is not within the destination region, transfer the mail piece to the distribution center within the destination region
94
If the distribution center is within the destination region, begin verifying the postage indicia by reading the digital signature and the key ID from the indicia
96
Use the key ID read from the indicia to retrieve the corresponding verification key from the table of all verification keys
98
Use the retrieved verification key to compute a digital signature for the indicia, and compare the computed digital signature with the digital signature from the postage indicia to verify the indicia
100

Verifying Postage Indicia

FIG. 6